Group Theory

Randy S

Abstract One of the simplest and most widely used mathematical concepts in physics is the concept of a group. Group theory is central to the study of symmetry. This article reviews some basic definitions in group theory.

Contents

1 What is a group?

A **group**[1] is a set G for which any two elements $a, b \in G$ may be composed to get a single element $a \circ b \in G$, subject to these rules:

- G includes a special element I called the **identity** such that $I \circ a = a \circ I = a$ for every element a.
- Every element a has an **inverse** a^{-1} such that $a \circ a^{-1} = a^{-1} \circ a = I$.
- Composition is **associative**: $(a \circ b) \circ c = a \circ (b \circ c)$.

That's all! The definition is easy, but group theory is still a wonderfully rich subject. This article reviews some of the concepts in group theory that are used often in physics. To get started, here is some basic vocabulary:

- Two elements a, b are said to **commute** with each other if $a \circ b = b \circ a$. A group in which all elements commute with each other is called **commutative**, also called **abelian**. Most groups are **noncommutative**, also called **nonabelian**.
- A subset $H \subset G$ is called a **subgroup** if it is a group all by itself, with the same composition $\circ$ and same identity element as G.
- A group G is called **finite** if it has a finite number of distinct elements. The number of elements is called the **order** of G, denoted $|G|$.

For abelian groups, addition and multiplication are both common ways of implementing the composition $\circ$, as illustrated in the next section. For nonabelian groups, the composition $\circ$ is almost always called *multiplication* and written using juxtaposition: ab instead of $a \circ b$. Most of this article follows that convention.

[1] Belk (2008) gives a concise online introduction to the idea of a group using Rubik's cube as an example. Beeler (2019) gives a less concise (but entertaining) introduction, again using Rubik's cube.

2 Examples of abelian groups

- The **additive group of real numbers**, denoted $\mathbb{R}$. This group consists of all real numbers, with addition as the composition: $a \circ b \equiv a + b$. The identity element is the number 0, and the "inverse" of r is its negative, $-r$.
- The **multiplicative group of nonzero real numbers**. This group consists of all nonzero real numbers, with multiplication as the composition: $a \circ b \equiv a \times b$. The identity element is the number 1, and the inverse of r is $1/r$.
- The **additive group of integers**, denoted $\mathbb{Z}$. This group consists of all integers, with addition as the composition. The identity element is the number 0, and the "inverse" of n is its negative, $-n$. This is a subgroup of the additive group of real numbers.
- The **multiplicative group of nonzero rational numbers**. This group consists of all nonzero rational numbers, with multiplication as the composition. The identity element is the number 1, and the inverse of r is $1/r$. This is a subgroup of the multiplicative group of real numbers.
- The **cyclic group** $\mathbb{Z}_N$, where N is a fixed positive integer. This group consists of the integers $\{0, 1, 2, ..., N-1\}$, and composition is addition modulo N. The identity element is the number 0. This group is finite, with order $|\mathbb{Z}_N| = N$.
- The **mutliplicative group of complex numbers z with absolute value** $|z| = 1$. The identity element is the number 1. This group is denoted $U(1)$.
- The **mutliplicative group of real numbers r with magnitude** $|r| = 1$. The identity element is the number 1. This group is finite, with only two elements, namely ± 1. This is a subgroup of $U(1)$.

3 Examples of nonabelian groups

- The **symmetric group** S_N. Each element of this group is (or can be faithfully represented by) a permutation of N objects – that is, as an invertible function from a set of N objects to itself. The composition $a \circ b$ is the function obtained by applying the functions a and b in succession. This group is finite, with order $|S_N| = N!$ (N factorial).[2] It is nonabelian if $N \geq 3$.

- The **alternating group** A_N. This is the subgroup of S_N consisting of all *even* permutations. A permutation is called **even** if it can be constructed as the composition of an even number of two-object swaps. This group has order $|A_N| = N!/2$. It is nonabelian if $N \geq 4$.

- The **general linear group** $GL(N, \mathbb{R})$. Each element of this group is an invertible $N \times N$ matrix whose components are real numbers, and the group includes all such matrices. Composition is matrix multiplication.[3] This group is nonabelian if $N \geq 2$.

- The **orthogonal group** $O(N)$. This is the subgroup of $GL(N, \mathbb{R})$ consisting of matrices M that satisfy $M^T = M^{-1}$ (transpose = inverse). It is nonabelian if $N \geq 3$.

- The **euclidean group** $E(N)$. This is the group of all isometries (distance-preserving transformations) of N-dimensional euclidean space. It can be (faithfully) represented as the group of matrices whose lower-right component is 1, whose other N components along the bottom row are zero, and whose upper-left $N \times N$ block belongs to $O(N)$. It is nonabelian if $N \geq 2$.

- The **unitary group** $U(N)$. Each element is a unitary matrix[4] of size $N \times N$, and the group includes all such matrices.

[2] $N! \equiv N \times (N-1) \times (N-2) \times \cdots \times 3 \times 2 \times 1$.

[3] https://www.mathsisfun.com/algebra/matrix-multiplying.html

[4] A matrix M of size $N \times N$ with complex components is called **unitary** if $M^\dagger = M^{-1}$, where $M^\dagger$ is the hermitian conjugate of M (article 18505).

4 Generating a finite group from a subset

Let G be a finite group. A subset $S \subset G$ (not necessarily a subgroup) is said to **generate** the group G if G does not have any subgroup (other than itself) that contains all of S. We can also say it like this: S **generates** G if every element of G can be expressed as a composition of elements of S. Examples:

- If N is prime and g is a non-identity element of the cyclic group $\mathbb{Z}_N$, then g generates $\mathbb{Z}_N$.
- If N is not prime and g is a non-identity element of the cyclic group $\mathbb{Z}_N$, then g may or may not generate $\mathbb{Z}_N$, depending on which element of g we choose.
- For any N, the symmetric group S_N is generated by the set of all two-object swaps (permutations that exchange two of the N objects and leave the others where they are).

More vocabulary: The **order** of an individual element $g \in G$ is defined to be the smallest integer n for which $g^n = I$, if any such integer exists. If N is prime, then any non-identity element $g \in \mathbb{Z}_N$ has order N. If $g \in S_N$ is a two-object swap, then g has order 2.

In the case of a **Lie group**[5] like $O(N)$ or $U(N)$, which has a continuum of elements, the word usually means something slightly different: elements of the group are *generated* by elements of the corresponding **Lie algebra**, which are not themselves elements of the group.[6]

[5] Chapter 7 in Lee (2013) introduces Lie groups. Appendix A in Harlow and Ooguri (2018) gives a more concise introduction.

[6] Fulton and Harris (1991)

5 The center

For any group G, the **center** of G consists of all elements of G that commute with everything in G. The center of G is denoted $Z(G)$, and it is a subgroup of G. Examples:

- If G is abelian, then $Z(G) = G$.
- The symmetric group S_N has **trivial** center, which means the center consists only of the identity element. In other words, the identity element is the only element in S_N that commutes with everything in S_N.
- For $N \geq 3$, the center of $O(N)$ consists of two elements, namely $\pm I$.
- The **special unitary group** $SU(N)$ is the subgroup of $U(N)$ consisting of unitary matrices whose determinant is equal to 1. The center of $SU(N)$ consists of multiples of the identity matrix I of the form $z^n I$ with $n \in \{0, 1, 2, ..., N-1\}$ and $z = e^{2\pi i/N}$. For motivation: the center of $SU(N)$ has been featured in attempts to understand the phenomenon of **confinement** in quantum chromodynamics.[7]

[7] This subject is reviewed in Greensite (2011) and Cohen (2013).

6 Homomorphism

Let G and H be groups. A map

$$G \xrightarrow{\sigma} H \qquad\qquad g \mapsto \sigma(g)$$

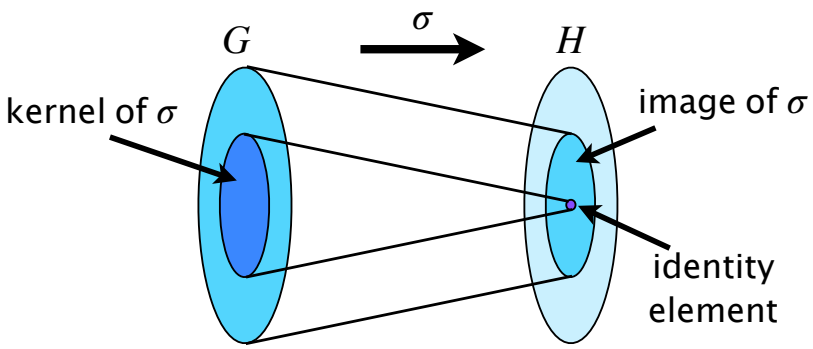
is called a **homomorphism** if it respects composition – that is, if

$$\sigma(g) \circ \sigma(g') = \sigma(g \circ g') \tag{1}$$

for all $g, g' \in G$. The subsets

$$\sigma(G) \subset H \qquad\qquad \sigma^{-1}(I) \subset G$$

are called the **image** and **kernel** of σ, respectively. These definitions are illustrated below, using concentric ellipses to represent groups and subgroups:



The kernel is a subgroup of G, and the image is a subgroup of H.[8]

Category theory emphasizes relationships (**morphisms**) between mathematical objects more than the internal structure of the objects themselves.[9] One important example of a category is the one whose objects are groups and whose morphisms are homomorphisms. This article doesn't go into category theory, but the concept of a homomorphism is still central to the rest of this article.

[8] Scott (1987), theorems 2.1.1 and 2.1.7

[9] Spivak (2013) and McLarty (1992) are relatively inviting introductions to category theory.

7 Isomorphism

Two groups G and H are called **isomorphic** denoted $G \cong H$, if there is a bijective (one-to-one) homomorphism from one to the other. Such a homomorphism is called an **isomorphism**. Loosely speaking, an isomorphism is a 1-to-1 correspondence between elements of G and elements of H that respects multiplication. Regarded as abstract groups, isomorphic groups are the "same" group, even though they may be represented differently. Examples:

- The abstract group called $U(1)$ may be described in more than one way, including these: (1) as the multiplicative group of complex numbers with magnitude 1, or (2) as the additive group of real numbers θ modulo 2π. These are isomorphic to each other as abstract groups, even though they're realized differently – one using multiplication, the other using addition. The complex number $e^{i\theta}$ in the multiplicative version corresponds to the real number θ in the additive version.

- The group $\mathbb{Z}_N$, defined as an additive group in section 2, is isomorphic to the center of $SU(2)$ (section 5), which is the multiplicative group that consists of complex numbers $e^{2\pi ik/N}$ with $k \in \{0, 1, 2, ..., N-1\}$.

An isomorphism from G to itself is called an **automorphism**. The set of all automorphisms of G is again a group, denoted $\mathrm{Aut}(G)$. We can think of this as the group of symmetries of the group G. Fun fact: non-isomorphic groups can have isomorphic automorphism groups.[10]

An **inner automorphism** is an automorphism of the form $G \to g^{-1}Gg$ for some $g \in G$. For those of us who are intrigued by exceptions, here's a fun result:[11] the symmetric group S_N has a non-inner automorphism if and only if $N = 6$.

The map that sends each element of G to its inverse is an example of an *anti*automorphism – like an automorphism except that it reverses the order of multiplication.

[10] Rotman (1995), example 7.3 (pages 156-157)

[11] Rotman (1995), theorem 7.5 (page 158) and theorem 7.9 (page 160).

8 Normal subgroups

If G is a group and σ a homomorphism from G to some other group, then the kernel of σ is the subset $K \subset G$ that gets mapped to the identity element (section 6). Section 6 mentioned that K must be a subgroup of G. In fact, K must be a special kind of subgroup called a **normal subgroup**. This relationship is denoted $K \triangleleft G$, and it has this property:[12] $K \triangleleft G$ if and only if $gKg^{-1} = K$ for all $g \in G$.

The relation $\triangleleft$ is not transitive. To see this, consider the euclidean group $E(2)$. This can be viewed as a matrix group in which each matrix has the form

$$\begin{bmatrix} c & s & a \\ -s & c & b \\ 0 & 0 & 1 \end{bmatrix} \tag{2}$$

with real-valued components a, b, c, s satisfying $c^2 + s^2 = 1$ (section 3). Let $T(2)$ be the subgroup for which $c = 1$ (which implies $s = 0$), and let $T(1)$ be the subgroup of $T(2)$ for which $b = 0$. Then $T(1) \triangleleft T(2) \triangleleft E(2)$, but $T(1)$ is not a normal subgroup of $E(2)$. This shows that the relation $\triangleleft$ is not transitive.

[12] Scott (1987), theorem 2.1.8 (page 26)

9 Quotient groups

Let G be a group and σ a homomorphism from G to some other group. Section 8 pointed out that the kernel $K \equiv \sigma^{-1}(I)$ must be a normal subgroup of G. What about the image $\sigma(G)$? The image is not a subgroup of G, but it is related to G and K in an important way: we can think of $\sigma(G)$ as G "modulo" K.

To make this idea precise, define the **quotient group** G/K (also called the **factor group**) by regarding each of the sets $gK \subset G$ to be a single element, with multiplication defined by $(g_1K)(g_2K) \equiv (g_1g_2K)$. This definition makes sense because K is a normal subgroup, which gives this identity in G:

$$g_1Kg_2K = g_1(g_2Kg_2^{-1})g_2K = g_1g_2KK = g_1g_2K.$$

The identity element of G/K corresponds to the set $K \subset G$. Theorem:[13] If $G \to H$ is a homomorphism with kernel K, then its image is isomorphic to G/K.

For an example of a quotient group, think about the original 3-layer Rubik's cube. The moves of this famous puzzle form a group G. The subgroup consisting of moves that don't affect the corners is a normal subgroup H. The factor group G/H corresponds to ignoring everything *except* the corners.[14]

Section 8 pointed out that the normal-subgroup relation $\triangleleft$ is not transitive in general, but suppose that $F \triangleleft K \triangleleft G$ and $F \triangleleft G$. In this case,[15]

$$\frac{G/F}{K/F} \cong \frac{G}{K}.$$

Here's a theorem[16] that highlights a relationship between the center $Z(G)$ of G and the automorphism group of G: for any group G, the set of all inner automorphisms is a normal subgroup of $\mathrm{Aut}(G)$, and it is isomorphic to $G/Z(G)$.

[13] Rotman (1995), theorem 2.23 (page 35)
[14] Beeler (2019), slide 53
[15] Scott (1987), theorem 2.3.6 (page 33)
[16] Rotman (1995), theorem 7.1 (page 156)

10 Simple groups

A group that doesn't have any nontrivial normal subgroups[17] is called **simple**. In other words, a group is called simple if it has no nontrivial homomorphisms into any other group,[18] so nontrivial factor groups cannot be formed. According to Gannon (2001),

> The finite simple groups are to group theory what the prime numbers are to number theory — in a sense they are the elementary building blocks of all finite groups.

Examples:

- If N is prime, then the cyclic group $\mathbb{Z}_N$ is simple. (It doesn't have any nontrivial subgroups at all, much less any nontrivial *normal* subgroups.)
- The alternating group A_5 is the smallest nonabelian finite simple group.[19] It is isomorphic to the group of rotational symmetries of a dodecahedron (or icosahedron). It has order $|A_5| = 60$. The next smallest nonabelian finite simple group has order 168.

The finite simple groups have been completely classified (up to isomorphism, of course).[20] Most of them fit into a few infinite sequences, but 26 of them don't: these are the **sporadic** finite simple groups.[20] The largest of the sporadic groups is called the **(Fischer-Griess) Monster**. For those of us who are intrigued by exceptions: Witten (2007) mentions a candidate for the "most natural known structure" having the Monster group as its symmetry group.

[17] By *nontrivial subgroup*, I mean a subgroup that has more than one element and is not the whole group.

[18] By *nontrivial homomorphism*, I mean a homomorphism whose kernel is a nontrivial subgroup.

[19] Madore (2003)

[20] Solomon (2018)

11 Representations

A **representation**[21] of a group G is a homomorphism of G into the group of all linear transformations of some vector space V, so that each element of G is represented by a specific linear transformation of V. A representation is called **faithful** if the kernel of the homomorphism consists only of the identity element, so that distinct elements of the group are represented by distinct linear transformations of V. A representation is called **irreducible** if V does not have any nontrivial subspace (other than the zero-dimensional subspace and V itself) that is self-contained under all transformations in the image of G. Otherwise, it is called **reducible**. Examples:

- For $a, b, c, d \in \mathbb{C}$ (the field of complex numbers), the map

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \to \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 1 \end{bmatrix} \tag{3}$$

  is a homomorphism from $SU(2)$ to the group of linear transformations of a 3d vector space V over $\mathbb{C}$. This representation is faithful, and it's reducible because the subspace spanned by the first two dimensions of V is self-contained under the transformations defined by the right-hand side of (3).

- The set of 2×2 traceless hermitian matrices

$$X = \begin{bmatrix} x_3 & x_1 + ix_2 \\ x_1 - ix_2 & -x_3 \end{bmatrix}$$

  with $x_1, x_2, x_3 \in \mathbb{R}$ is a 3d vector space V over $\mathbb{R}$ (the field of real numbers). Each $M \in SU(2)$ defines a linear transformation of V as $X \to MXM^\dagger$. This representation of $SU(2)$ is irreducible, but it's not faithful: for any $M \in SU(2)$, the elements $\pm M$ are both mapped to the same transformation of V. For motivation: in quantum theory, this example is associated with the description of a **spin 1/2** particle in 3d space.

[21] Fulton and Harris (1991)

12 Extensions

Given any two groups K and Q, their **direct product** $K \times Q$ is defined like this: an element of $K \times Q$ is a pair (k, q) with $k \in K$ and $q \in Q$, with multiplication defined by

$$(k_1, q_1)(k_2, q_2) = (k_1 k_2, q_1 q_2).$$

Clearly, $K \times 1 \cong K$ is a normal subgroup of $K \times Q$, and the quotient group $(K \times Q)/(K \times 1)$ is isomorphic to Q. Given two groups K and Q, what other groups G contain K as a normal subgroup with $Q = G/K$?[22] In other words, for what groups G does a homomorphism exist whose kernel is K and whose image is Q? This question leads to the study of group *extensions*. At least one such group always exists, namely the direct product $K \times Q$, which is called the **trivial** extension. The theory of extensions seeks to classify and construct nontrivial examples.

A sequence of homomorphisms is called **exact** if the image of each homomorphism is the kernel of the next one. An exact sequence of the form[23]

$$1 \longrightarrow K \longrightarrow G \xrightarrow{\beta} Q \longrightarrow 1 \tag{4}$$

is called a **short exact sequence**, illustrated graphically in figure 1. In this case,

- The kernel K of β is isomorphic to a subgroup of G, which will also be denoted by K.
- The image Q of β is isomorphic to the quotient group G/K.
- The group G, together with the homomorphisms entering and leaving it, is called an **extension** of Q by K. (Some authors call it an "extension of K by Q," so I prefer to let the arrow-diagram speak for itself.)

The next section shows examples of nontrivial extensions.

[22] I'm using the letters K and Q for Kernel and Quotient, respectively.

[23] The symbol 1 denotes the trivial group, which has only the identity element.

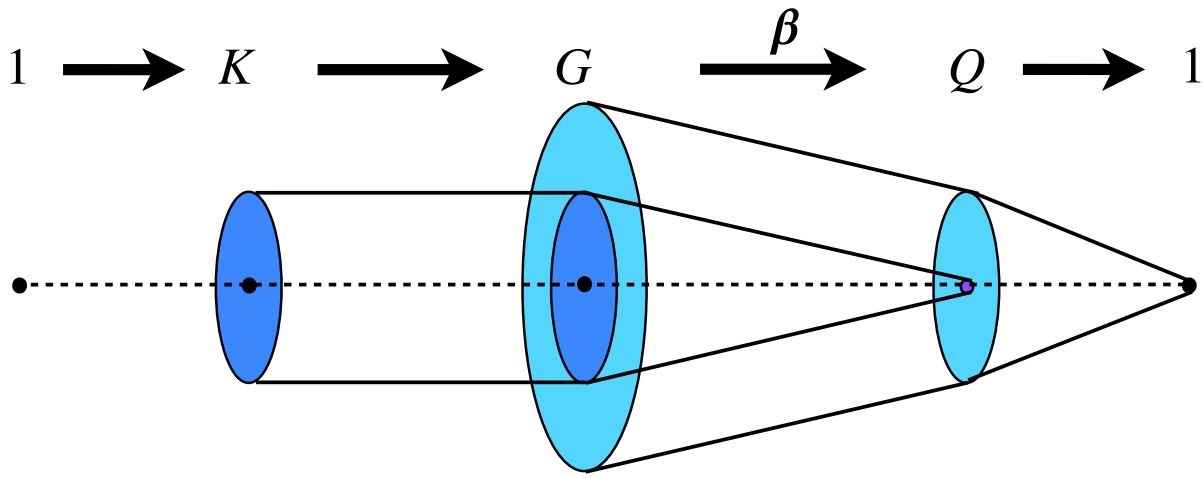


Figure 1 – Graphic depiction of the short exact sequence (4). The dashed line represents the fact that the identity element is always mapped to the identity element. The solid lines indicate how the other elements are mapped.

13 Split extensions

An extension (4) is called **split** if there is a homomorphism $Q \xrightarrow{\alpha} G$ such that the composite map $Q \xrightarrow{\alpha} G \xrightarrow{\beta} Q$ is the identity map. Then G is equivalent (section 14) to a **semidirect product** of K and Q.[24] This is a generalization of the direct product. An extension in which the elements of $K \triangleleft G$ commute with all elements of G is called a **central** extension. If an extension is both central and split, then it is trivial (in other words, it's a direct product).[25]

Here's an example of a split extension, using notation that was introduced in sections 3 and 8:

$$1 \longrightarrow T(2) \longrightarrow E(2) \longrightarrow O(2) \longrightarrow 1$$

where β sets $a = b = 0$ in (2). This is a split extension (semidirect product),[26] but it is not a direct product: $E(2) \ncong T(2) \times O(2)$. Another example: the Poincaré group is a split extension of the Lorentz group by the group of translations in spacetime.

In contrast, an extension of the form

$$1 \longrightarrow \mathbb{Z}_2 \longrightarrow \mathbb{Z}_4 \xrightarrow{\beta} \mathbb{Z}_2 \longrightarrow 1,$$

cannot be a split extension. To see this, use the fact that $\mathbb{Z}_4$ is isomorphic to the multiplicative group with elements $\{\pm 1, \pm i\}$, with $i^2 = -1$, and $\mathbb{Z}_2$ is isomorphic to the multiplicative group with elements $\{\pm 1\}$. The only short exact sequence of the form shown above is the one defined by the homomorphism $\beta(z) = z^2$. If the extension were split, then we would need a homomorphism $\alpha : \{\pm 1\} \to \{\pm 1, \pm i\}$ satisfying $\beta(\alpha(-1)) = -1$. That implies $(\alpha(-1))^2 = -1$, but if α were a homomorphism then we would have $(\alpha(-1))^2 = \alpha((-1)^2) = \alpha(1) = 1$. That's a contradiction, so the extension shown above cannot be a split extension.

[24] Scott (1987), theorem 9.5.4 (page 242). The semidirect product is defined in Rotman (1995), chapter 7, page 167.

[25] Schottenloher (2008), lemma 3.20 (page 57)

[26] To see that it is split, let α be the map that identifies $O(2)$ with the subgroup of $E(2)$ leaving the origin unmoved.

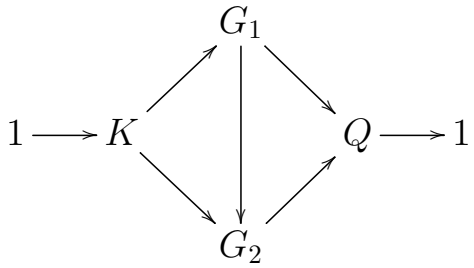
14 Equivalence of extensions

Two extensions

$$1 \longrightarrow K \longrightarrow G_1 \longrightarrow Q \longrightarrow 1$$

$$1 \longrightarrow K \longrightarrow G_2 \longrightarrow Q \longrightarrow 1$$

are called **equivalent** if there is a homomorphism $G_1 \to G_2$ that makes the following diagram commute:[27]



Such a homomorphism is always an isomorphism.[28]

Two extensions can be inequivalent even if they involve the same triple of groups.[29] For this reason, to specify an extension unambiguously, we should specify the groups *and* the homomorphisms.

[27] A diagram whose arrows are homomorphisms is said to **commute** if all paths from A to B shown in the diagram define the same composite homomorphism $A \to B$.

[28] Scott (1987), theorem 9.1.6 (page 211)

[29] Scott (1987), exercise 9.1.13 (page 212)

15 References

Beeler, 2019. "Group Theory and the Rubik's Cube" http://faculty.etsu.edu/beelerr/rubik-talk2.pdf

Belk, 2008. "Puzzles, Groups, and Groupoids" https://cornellmath.wordpress.com/2008/01/27/puzzles-groups-and-groupoids/

Cohen, 2013. "Center Symmetry and Confinement" https://indico.cern.ch/event/195077/contributions/1473970/

Fulton and Harris, 1991. *Representation Theory: A First Course*. Springer

Gannon, 2001. "Postcards from the edge, or snapshots of the theory of generalized moonshine" https://arxiv.org/abs/math.QA/0109067

Greensite, 2011. *An Introduction to the Confinement Problem*. Springer

Harlow and Ooguri, 2018. "Symmetries in Quantum Field Theory and Quantum Gravity" https://arxiv.org/abs/1810.05338

Lee, 2013. *Introduction to Smooth Manifolds (Second Edition)*. Springer

Madore, 2003. "Orders of non abelian simple groups" http://www.madore.org/~david/math/simplegroups.html

McLarty, 1992. *Elementary Categories, Elementary Toposes*. Clarendon Press

Rotman, 1995. *An Introduction to the Theory of Groups*. Springer-Verlag

Schottenloher, 2008. "Central Extensions of Groups." Pages 39-62 in *A Mathematical Introduction to Conformal Field Theory*, edited by Schottenloher (Lecture Notes in Physics 759)

Scott, 1987. *Group Theory*. Dover

Solomon, 2018. "The Classification of Finite Simple Groups: A Progress Report" *Notices of the AMS* **65**: 646-651, https://www.ams.org/journals/notices/201806/rnoti-p646.pdf

Spivak, 2013. "Category Theory for Scientists" https://ocw.mit.edu/courses/mathematics/18-s996-category-theory-for-scientists-spring-2013/textbook

Witten, 2007. "Three-Dimensional Gravity Reconsidered" https://arxiv.org/abs/0706.3359

16 References in this series

Article **18505** (https://cphysics.org/article/18505):
"Matrix Math" (version 2023-02-12)